Notice of Allowability	Application No.	Applicant(s)	
	09/534,916	MARSH, DAVID J.	
	Examiner	Art Unit	
	Seung H. Lee	2876	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *27 April 2006*.

2. ☒ The allowed claim(s) is/are *1-22,24-36,38-46,50 and 52-57*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20060711* .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. Receipt is acknowledged of the response filed on 27 April 2006, which has been entered in the file.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Allan Sponseller (REG. NO. 38,318) on November July 11, 2006.

The application has been amended as follows:

Claims 16, 29, 40, 45, and 50 have been amended as follows:

(see the version with markings to show changes made, attached)

16. (Currently amended) A method of encrypting all media content received at a user's home from a programming source, the method comprising:

checking, at the user's home, whether a smart card is authorized to encrypt the media content; and

encrypting, at the user's home using a key that is a combination of a household identifier associated with the user's home and a private key of a private key/public key pair, the media content regardless of whether the received media content was received scrambled, but only if the smart card is authorized to encrypt the media content.

29. (Currently amended) A method of allowing parental control over media content, the method comprising:

receiving, at a household, media content;

encrypting, at the household, all of the received media content using a key corresponding to a smart card regardless of whether the received media content was received scrambled, wherein the key comprises a combination of a household identifier ~~is~~ associated with one household and a private key of a private key/public key pair; and

requiring the smart card to be present to decrypt and render the media content.

40. (Currently amended) A smart card comprising:

a key, associated with one particular household, to be used to encrypt and decrypt media content associated with the one particular household at the one particular household but not to encrypt and decrypt media content associated with other households, wherein the key is to encrypt all the media content associated with the one particular household without regard for whether the media content was received scrambled, and wherein the key comprises a combination of a household identifier of the one particular household and a private key of a private key/public key pair; and

a user-specific information storage section to store user preferences.

45. (Currently amended) A method comprising:

maintaining, on an integrated circuit card, information regarding a user's preferences corresponding to media content; and

maintaining, on the integrated circuit card, a key to be used to encrypt and decrypt media content associated with one particular household at the one particular household but not to encrypt and decrypt media content associated with other households, wherein the key is to be used to encrypt all the media content associated with the one particular household without regard for whether the media content was received scrambled, and wherein the key is a combination of a household identifier of the one particular household and a private key of a private key/public key pair.

50. (Currently amended) A method of identifying boundaries of a network of devices, the method comprising:

encrypting, at a single house using a key that is a combination of a household identifier and a private key of a private key/public key pair, media content based on an identifier corresponding to a plurality of smart cards regardless of whether the media content is received scrambled; and

limiting rendering of the media content to a network of devices to which the plurality of smart cards are coupled, wherein the network of devices is maintained within the single house.

Allowable Subject Matter

3. Claims 1-22, 24-36, 38-46, 50, and 52-57 have been allowed over the prior art of record.

4. The following is an examiner's statement of reasons for allowance:

Blatter et al. (US 5,933,500) discloses a decoding system for generating program in encrypted/decrypted form using the smart card,

Handelman et al. (US 5,666,412) discloses a CATV system having a plurality of smart card reader/receptacles therewith for descramble program channel according to data stored in the smart card,

Yoshida et al. (US 6,411,712) discloses a digital broadcast receiver wherein the receiver can encrypt/decrypt broadcast signals using the smart card.

However, Blatter et al., Handelman et al., and Yoshida et al. taken alone or in combination thereof fail to specifically teach that a smart card or integrated circuit card comprising a key for encrypting and decrypting media content wherein the key is combination of the household identifier and a private key and public key pair as set forth in the claims.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communication from the examiner should be directed to Seung H. Lee whose telephone number is (703) 308-5894. The examiner can normally be reached on Monday to Friday from 7:30 AM to 4:00 PM.

If attempt to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee, can be reached on (703) 305-3503. The fax-phone number for this group is (703) 308-5841 or (703) 308-7722.

Communications via Internet e-mail regarding this application, other than those under 35 U.S.C. 132 or which otherwise require a signature, may be used by the applicant and should be addressed to [**michael.lee@uspto.gov**].

All Internet e-mail communications will be made of record in the application file. PTO employees do not engage in Internet communications where there exists a possibility that sensitive information could be identified or exchanged unless the record includes a properly signed express waiver of the confidentiality requirements of 35 U.S.C. 122. This is more clearly set forth in the Interim Internet Usage Policy published in the Official Gazette of the Patent and Trademark on February 25, 1997 at 1195 OG 89.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 308-0956.

SEUNG HO LEE
PRIMARY EXAMINER

Version with markings to show changes made

1. (Previously presented) A smart card comprising:

a key, associated with a household, to be used to encrypt and decrypt media content at the household that is associated with the household, the key being a combination of a household identifier and a private key of a private key/public key pair; and

a memory unit, the memory unit including,

a user-specific information storage section to store user preferences, and

a data storage section to store data that is expected to be of value to a user.

2. (Original) A smart card as recited in claim 1, wherein the memory unit comprises a nonvolatile memory.

3. (Original) A smart card as recited in claim 1, wherein the data comprises electronic money.

4. (Original) A smart card as recited in claim 3, wherein the smart card can be used to encrypt and decrypt media content only if at least a threshold amount of electronic money is stored on the smart card.

5. (Original) A smart card as recited in claim 1, wherein the smart card corresponds to a particular category of media content and is used to encrypt and decrypt only that particular category of media content.

6. (Original) A smart card as recited in claim 5, wherein one of the categories of media content comprises family-oriented media content and another of the categories of media content comprises adult-oriented media content.

7. (Original) A smart card as recited in claim 1, wherein the memory unit further includes a rating associated with the smart card that is used to compare the rating with a rating corresponding to the media content and determine, based on the comparison, whether to allow access to the media content.

8. (Original) A smart card as recited in claim 1, wherein the smart card is used to limit where rendering of the media content can occur.

9. (Previously presented) A smart card comprising:

a private key of a private key/public key pair;

a household identifier, associated with one particular household, to be combined with the private key, and the combined value to be used to encrypt and decrypt media content that is associated with the one particular household and that is to be rendered

at the one particular household, but not to encrypt and decrypt media content associated with other households; and

a data storage section to store data that is expected to be of value to a user.

10. (Original) A smart card as recited in claim 9, further comprising a communications module to communicate, to a computing device module that encrypts media content, an indication of whether to encrypt the media content based on data stored in the data storage section.

11. (Original) A smart card as recited in claim 9, further comprising a communications module to communicate, to a computing device module that decrypts media content, an indication of whether to decrypt the media content based on data stored in the data storage section.

12. (Original) A smart card as recited in claim 9, further comprising a processor to execute instructions to encrypt and decrypt the media content.

13. (Original) A smart card as recited in claim 9, wherein the data storage section is maintained in a nonvolatile memory.

14. (Original) A smart card as recited in claim 9, further comprising a user-specific information storage section to store user preferences.

15. (Original) A smart card as recited in claim 9, wherein the data in the data storage section comprises electronic money.

16. (Currently amended) A method of encrypting all media content received at a user's home from a programming source, the method comprising:

checking, at the user's home, whether a smart card is authorized to encrypt the media content; and

encrypting, at the user's home using a key that is a combination of a household identifier associated with the user's home and a private key of a private key/public key pair, the media content regardless of whether the received media content was received scrambled, but only if the smart card is authorized to encrypt the media content.

17. (Original) A method as recited in claim 16, further comprising determining that the smart card is authorized to encrypt the media content if at least a threshold amount of electronic money is available on the smart card.

18. (Original) A method as recited in claim 16, further comprising determining that the smart card is authorized to encrypt the media content only if data is stored on the smart card that is expected to be of value to a user.

19. (Original) A method as recited in claim 16, further comprising:

checking whether the smart card is authorized to decrypt media content; and

decrypting the media content only if the smart card is authorized to decrypt the media content.

20. (Original) One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 16.

21. (Previously presented) A method of decrypting media content, the method comprising:

checking whether a portable integrated circuit device is authorized to decrypt the media content, wherein the portable integrated circuit device stores a decryption key and additional data, and wherein the decryption key is a combination of a household identifier and a private key of a private key/public key pair;

determining that the portable integrated circuit device is authorized to decrypt the media content only if data other than electronic money is stored as the additional data on the portable integrated circuit device, wherein the data is expected to be of value to a user, and wherein the data is not used to decrypt the media content; and

decrypting the media content only if the portable integrated circuit device is authorized to decrypt the media content.

22. (Previously presented) A method as recited in claim 21, further comprising determining that the portable integrated circuit device is authorized to decrypt the media

content if at least a threshold amount of electronic money is available on the portable integrated circuit device.

23. (Canceled).

24. (Previously presented) A method as recited in claim 21, further comprising:

checking whether the portable integrated circuit device is authorized to encrypt media content; and

encrypting the media content only if the portable integrated circuit device is authorized to encrypt the media content.

25. (Original) One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 21.

26. (Previously presented) A system comprising:

a plurality of smart cards, each to be used for encrypting different categories of multimedia presentations; and

an encryption module coupled to receive a multimedia presentation and encrypt, at the user's home, the multimedia presentation based on a combination of a household identifier and a private key of a private key/public key pair maintained on one of the plurality of smart cards.

27. (Previously presented) A system as recited in claim 26, further comprising a decoding module, coupled to receive the encrypted multimedia presentation, decrypt the encrypted multimedia presentation, decode the decrypted multimedia presentation, and transmit the decoded multimedia presentation to a rendering module.

28. (Previously presented) A system as recited in claim 26, wherein one of the categories of multimedia presentations comprises family-oriented media content and another of the categories of multimedia presentations comprises adult-oriented media content.

29. (Currently amended) A method of allowing parental control over media content, the method comprising:

receiving, at a household, media content;

encrypting, at the household, all of the received media content ~~based on~~ using a key ~~household identifier~~ corresponding to a smart card regardless of whether the received media content was received scrambled, wherein the key comprises a combination of a household identifier ~~is~~ associated with one household and a private key of a private key/public key pair; and

requiring the smart card to be present to decrypt and render the media content.

30. (Original) A method as recited in claim 29, wherein the requiring comprises requiring the smart card to be inserted into a smart card reader coupled to a computing device that is decrypting the media content.

31. (Original) A method as recited in claim 29, further comprising using a plurality of different smart cards to encrypt and decrypt media content, each of the plurality of smart cards corresponding to a different category of media content.

32. (Original) A method as recited in claim 31, wherein one of the categories of media content comprises family-oriented media content and another of the categories of media content comprises adult-oriented media content.

33. (Original) One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 29.

34. (Previously presented) A method of allowing parental control over media content, the method comprising:

comparing a rating corresponding to the media content to a rating associated with a smart card; and

allowing access to the media content if the rating corresponding to the media content does not exceed the rating associated with the smart card, wherein a plurality of ratings do not exceed the rating associated with the smart card, and wherein the

allowing access comprises allowing the media content to be encrypted using a combination of a household identifier and a private key of a private key/public key pair, at a user's home, for subsequent processing.

35. (Previously presented) A method as recited in claim 34, wherein the comparing comprises comparing the rating corresponding to the media content to the rating associated with the smart card as stored on the smart card.

36. (Original) A method as recited in claim 34, wherein the allowing access comprises allowing the media content to be decrypted for rendering.

37. (Canceled).

38. (Previously presented) One or more computer-readable media having stored thereon a computer program that, when executed by a computing device, causes the computing device to perform acts including:

receiving, at a household, media content;

controlling, at the household, encryption of the received media content based on a combination of a household identifier and a private key of a private key/public key pair corresponding to a smart card; and

maintaining user preferences information on the smart card, the user preferences information being available only when the smart card is coupled to the computing device.

39. (Original) One or more computer-readable media as recited in claim 38, wherein the smart card is coupled to the computing device when the smart card is inserted into a smart card reader that is coupled to the computing device.

40. (Currently amended) A smart card comprising:

a key, associated with one particular household, to be used to encrypt and decrypt media content associated with the one particular household at the one particular household but not to encrypt and decrypt media content associated with other households, wherein the key is to encrypt all the media content associated with the one particular household without regard for whether the media content was received scrambled, and wherein the key comprises a combination of a household identifier of the one particular household and a private key of a private key/public key pair; and

a user-specific information storage section to store user preferences.

41. (Original) A smart card as recited in claim 40, further comprising a communications module to communicate, to a computing device module that encrypts media content, the user preferences stored in the user-specific information storage section.

42. (Original) A smart card as recited in claim 40, further comprising a processor to manage the user-specific information storage section.

43. (Original) A smart card as recited in claim 40, wherein the user-specific information storage section is maintained in a nonvolatile memory.

44. (Original) A smart card as recited in claim 40, further comprising a data storage section to store data that is expected to be of value to a user.

45. (Currently amended) A method comprising:

maintaining, on an integrated circuit card, information regarding a user's preferences corresponding to media content; and

maintaining, on the integrated circuit card, a key to be used to encrypt and decrypt media content associated with one particular household at the one particular household but not to encrypt and decrypt media content associated with other households, wherein the key is to be used to encrypt all the media content associated with the one particular household without regard for whether the media content was received scrambled, and wherein the key is a combination of a household identifier of the one particular household and a private key of a private key/public key pair.

46. (Original) One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 45.

47. (Canceled).

48. (Canceled).

49. (Canceled).

50. (Currently amended) A method of identifying boundaries of a network of devices, the method comprising:

encrypting, at a single house using a key that is a combination of a household identifier and a private key of a private key/public key pair, media content based on an identifier corresponding to a plurality of smart cards regardless of whether the media content is received scrambled; and

limiting rendering of the media content to a network of devices to which the plurality of smart cards are coupled, wherein the network of devices is maintained within the single house.

51. (Canceled).

52. (Previously presented) A method as recited in claim 50, wherein the network devices include devices to receive media content and devices to render media content.

53. (Previously presented) A method as recited in claim 50, wherein one of the plurality of smart cards is coupled to a device when the smart card is inserted into a smart card reader coupled to the device.

54. (Previously presented) A method as recited in claim 50, wherein the plurality of smart cards can be moved to different devices to alter the boundaries of the network.

55. (Previously presented) A smart card as recited in claim 1, wherein the user preferences comprise one or more channels preferred by the user.

56. (Previously presented) A smart card as recited in claim 1, wherein the user preferences comprise one or more viewing times preferred by the user.

57. (Previously presented) A smart card as recited in claim 1, wherein the user preferences comprise one or more types of content preferred by the user.